The Open University
Mathematics and Computing: A Third Level Course
M381 Number Theory and Mathematical Logic
M381NTHB

M381
Number Theory Handbook

NOTE: This *Handbook* may be taken into the *M381* examination. However, no annotation is permitted other than the correction of errors and the highlighting or underlining of passages.

CONTENTS

Notation 3
Glossary 4
Results 9
Unit 1 Foundations 9
Unit 2 Prime Numbers 10
Unit 3 Congruence 12
Unit 4 Fermat's and Wilson's Theorems 14
Unit 5 Multiplicative Functions 15
Unit 6 Quadratic Reciprocity 17
Unit 7 Continued Fractions 19
Unit 8 Diophantine Equations 21
Appendix: Table of Primes 24
Cumulative Index of Units 26

Copyright © 1996 The Open University
SUP 30666 6
1.4

NOTATION

Some of the notation used in the course is listed below. A reference in the right-hand column refers to the unit (bold) and page number where the term first appears. This referencing system is followed throughout the Handbook.

F_n	the nth Fibonacci number	**2**	28
F_n	the nth Fermat number	**5**	16
M_p	the Mersenne number $2^p - 1$	**5**	12
$\mathbb{Q}$	the set of rational numbers	**1**	13
$\mathbb{R}$	the set of real numbers	**1**	13
R_n	the repunit consisting of n 1's	**5**	22
T_n	the nth triangular number	**1**	7
$\mathbb{Z}$	the set of integers	**1**	12
$\mathbb{Z}^+$	the set of positive integers	**1**	12
$\mathbb{Z}_n$	the set of equivalence classes modulo n, i.e. the set $\{0, 1, 2, \ldots, n-1\}$ with addition and multiplication modulo n	**3**	10
$a \mid b$	a divides b	**1**	22
$a \nmid b$	a does not divide b	**1**	22
$a \equiv b \pmod{n}$	a is congruent modulo n to b	**3**	6
$a \not\equiv b \pmod{n}$	a is incongruent modulo n to b	**3**	6
(a/p)	the Legendre symbol; see Glossary	**6**	12
$\lvert n \rvert$	the absolute value of n	**1**	13
$\mathrm{frac}(x)$	the fractional part of x	**7**	27
$\gcd(a, b)$	the greatest common divisor of a and b	**1**	23
$\mathrm{int}(x)$	the integer part of x	**6**	18
$\mathrm{lcm}(a, b)$	the least common multiple of a and b	**1**	28
$\mathrm{Li}(x)$	the logarithmic integral	**2**	25
$\min\{a, b\} = \begin{cases} a, & \text{if } a \leq b \\ b, & \text{otherwise} \end{cases}$	the minimum of a and b	**2**	12
$\max\{a, b\} = \begin{cases} a, & \text{if } a \geq b \\ b, & \text{otherwise} \end{cases}$	the maximum of a and b	**2**	13
$\pi(x)$	the number of primes less than or equal to x	**2**	25
$\phi(n)$	Euler's ϕ-function; see end of Glossary	**5**	18
$\sigma(n)$	the σ function; see end of Glossary	**5**	6
$\tau(n)$	the τ function; see end of Glossary	**2**	13
$[a_1, a_2, \ldots, a_n]$	the finite continued fraction with partial quotients $a_1, a_2, \ldots, a_n$	**7**	7
$[a_1, a_2, a_3, \ldots]$	the infinite continued fraction with partial quotients a_1, a_2, a_3, ...	**7**	20
$[a_1, a_2, \ldots, a_n, \langle b_1, b_2, \ldots, b_m \rangle]$	a periodic continued fraction with a cycle of length m	**7**	24

GLOSSARY

abundant numbers An integer n is abundant if $\sigma(n) > 2n$. **5** 34

amicable pair Integers m and n form an amicable pair if $\sigma(m) = \sigma(n) = m + n$. **5** 34

arithmetic progression/arithmetic series An arithmetic series is a series of the form **1** 7

$$a + (a + d) + (a + 2d) + (a + 3d) + \cdots$$

with a common difference d from one term to the next. The terms are said to be in arithmetic progression.

complete set of residues A complete set of residues modulo n consists of one element from each of the n residue classes. **3** 9

composite An integer $n > 1$ which is not prime is said to be composite. **2** 5

congruence modulo n An integer a is said to be congruent modulo n to integer b if the difference $a - b$ is divisible by n. We write $a \equiv b \pmod{n}$. If the difference $a - b$ is not divisible by n then a is incongruent modulo n to b. **3** 6

convergent The convergents of the FCF $[a_1, a_2, a_3, \ldots, a_n]$ are the values of the finite continued fractions **7** 11

$$[a_1], \quad [a_1, a_2], \quad [a_1, a_2, a_3], \quad \ldots, \quad [a_1, a_2, a_3, \ldots, a_n].$$

These are given by $[a_1, a_2, a_3, \ldots, a_k] = \dfrac{p_k}{q_k}$, where the numerators $p_1, p_2, \ldots, p_n$ and denominators $q_1, q_2, \ldots, q_n$ are given by

$$p_1 = a_1, \quad p_2 = a_1 a_2 + 1, \quad p_k = a_k p_{k-1} + p_{k-2}, \quad \text{for } 3 \le k \le n;$$
$$q_1 = 1, \quad q_2 = a_2, \quad q_k = a_k q_{k-1} + q_{k-2}, \quad \text{for } 3 \le k \le n.$$

The first n convergents of the ICF $[a_1, a_2, a_3, \ldots, a_n, \ldots]$ are the convergents of $[a_1, a_2, a_3, \ldots, a_n]$.

cycle (of a decimal fraction) In a decimal fraction, a block of digits which repeats indefinitely is called a cycle of the fraction. The number of digits in the cycle is the cycle length. **4** 10

cycle (of a periodic continued fraction) The block of partial quotients which repeats indefinitely in a periodic ICF is called the cycle of the ICF. The number of partial quotients in the cycle is the cycle length. **7** 24

deficient number An integer n is deficient if $\sigma(n) < 2n$. **5** 34

degree of a polynomial congruence If **4** 22

$$P(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0$$

is an integral polynomial then $P(x)$ has degree k modulo n if, after removing all terms, where $c_i \equiv 0 \pmod{n}$, the leading term remaining is $c_k x^k$.

If every coefficient $c_i \equiv 0 \pmod{n}$, then the polynomial is not assigned a degree modulo n.

The degree of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ is the degree of $P(x)$ modulo n.

divisor The integer a is divisible by the positive integer b if there exists an integer q such that $a = bq$. In this case b is said to be a divisor of a, and that a is a multiple of b. **1** 22

FCF FCF is an abbreviation for simple finite continued fraction. **7** 8

Fermat numbers The Fermat numbers are those integers of the form **5** 16

$$2^{2^n} + 1, \quad \text{for any integer } n \ge 0.$$

Fibonacci numbers The sequence of Fibonacci numbers **2** 27

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

is defined by

$$F_1 = 1, \quad F_2 = 1, \quad F_n = F_{n-1} + F_{n-2}, \quad \text{for } n > 2.$$

finite continued fraction A finite continued fraction is a finite expression (which can be evaluated) **7** 7

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{}{a_{n-1} + \cfrac{1}{a_n}}}},$$

where a_1 is any real number and the others, $a_2, a_3, \ldots, a_n$, are positive real numbers. The finite continued fraction is written symbolically as $[a_1, a_2, a_3, \ldots, a_n]$.

fractional part The fractional part of a real number x, denoted by $\text{frac}(x)$, is defined by **7** 27

$$x = \text{int}(x) + \text{frac}(x)$$

where $\text{int}(x)$ is the integer part of x.

fundamental solution The fundamental solution of Pell's equation, **8** 9

$$x^2 - ny^2 = 1,$$

is the unique solution in which x and y take their smallest positive values.

geometric series A geometric series **1** 16

$$a + ar + ar^2 + ar^3 + \cdots$$

is one in which the ratio of successive terms is constant.

greatest common divisor (gcd) The greatest common divisor of two integers a and b, not both of which are zero, is the positive integer n satisfying **1** 23

(a) n divides a, and n divides b;

(b) if d divides both a and b then $d \leq n$.

hexagonal numbers The hexagonal numbers form the sequence **1** 9

$$1, \quad 1+5, \quad 1+5+9, \quad 1+5+9+13, \quad \ldots$$

arising from arrangements of dots forming hexagons.

ICF ICF is an abbreviation for simple infinite continued fraction. **7** 20

infinite continued fraction Extending the notation for finite continued fractions, an infinite continued fraction is an unending expression $[a_1, a_2, a_3, \ldots]$ where a_1 is any real number and the others, $a_2, a_3, \ldots$, are positive real numbers. The value of the infinite continued fraction is the limit of the sequence of values **7** 20

$$[a_1], \quad [a_1, a_2], \quad [a_1, a_2, a_3], \quad \ldots, \quad [a_1, a_2, a_3, \ldots, a_n], \quad \ldots.$$

integer combination If a and b are integers, then any integer of the form **1** 24

$$ma + nb, \quad m, n \in \mathbb{Z}$$

is an integer combination of a and b.

integer part The integer part of a real number x, denoted $\text{int}(x)$, is the largest integer which does not exceed x. That is, **6** 18

$$\text{int}(x) \leq x < \text{int}(x) + 1.$$

integral polynomial An integral polynomial is a polynomial **3** 16

$$P(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$$

in which the coefficients $c_0, c_1, c_2, \ldots, c_m$ and the variable x are integers.

leading term The leading term of a polynomial is the non-zero term involving the highest power of x. **4** 22

least absolute residue The least absolute residue in a residue class modulo n is the unique integer x in the class which lies in the range $-\frac{n}{2} < x \leq \frac{n}{2}$. The n such numbers x form the set of least absolute residues modulo n. **3** 9

least common multiple (lcm) The least common multiple of the non-zero integers a and b is the positive integer n satisfying **1** 28

(a) a divides n, and b divides n;

(b) if a divides m and b divides m then $n \leq |m|$.

least positive residue The least positive residue in a residue class modulo n is the smallest non-negative integer belonging to the class. The set of least positive residues modulo n is the set $\{0, 1, 2, \ldots, n-1\}$. **3** 9

Legendre symbol If $\gcd(a, p) = 1$, where p is an odd prime, then the Legendre symbol (a/p) is defined by **6** 12

$$(a/p) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p, \\ -1, & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

linear congruence A linear congruence is a congruence of the form **3** 18

$$ax \equiv b \pmod{n},$$

where a and b are integers and n is a positive integer.

linear Diophantine equation The linear Diophantine equation is the equation **1** 34

$$ax + by = c, \quad \text{where } a, b, \text{ and } c \in \mathbb{Z},$$

which is to be solved in integers.

Mersenne prime The numbers of the form $M_p = 2^p - 1$, where p is prime, are called Mersenne numbers. If M_p happens to be prime, it is a Mersenne prime. **5** 12

method of infinite descent The method of infinite descent is a method of proof which uses the fact that a strictly decreasing sequence of positive integers must terminate. Typically it is used to prove that a Diophantine equation can have no solutions by showing that the existence of any positive solution leads to a second, strictly smaller, positive solution; an impossible situation. **8** 20

multiple The integer a is said to be a multiple of integer b if there exists an integer q such that $a = bq$; that is, if b is a divisor of a. **1** 22

multiplicative function A number-theoretic function f is said to be multiplicative if, for any number with prime decomposition $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ we have **5** 7

$$f(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = f(p_1^{k_1}) f(p_2^{k_2}) \ldots f(p_r^{k_r}).$$

non-negative A real number x is non-negative if it satisfies $x \geq 0$. **1** 33

number-theoretic function A function $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$, with the set of positive integers as domain and which takes integer values, is said to be a number-theoretic function. **5** 5

order of an integer modulo n If $\gcd(a, n) = 1$, then the order of a modulo n is defined to be the least positive integer c such that $a^c \equiv 1 \pmod{n}$. **5** 20

parity The parity of an integer depends on whether it is divisible by 2. It is either an odd integer (odd parity) or an even integer (even parity). **8** 13

partial quotient In a continued fraction $[a_1, a_2, a_3, \ldots]$, whether finite or infinite, the numbers $a_1, a_2, a_3, \ldots$, are called the partial quotients. **7** 7

pentagonal numbers The pentagonal numbers form the sequence **1** 9

$$1, \quad 1+4, \quad 1+4+7, \quad 1+4+7+10, \quad \ldots,$$

which arise from arrangements of dots in pentagons.

perfect number A perfect number is one which is equal to the sum of its divisors, excluding itself. To be precise, n is perfect if, and only if, $\sigma(n) = 2n$. **5** 11

periodic continued fraction An infinite continued fraction in which, from some point onwards, a block of partial quotients repeats indefinitely, is said to be periodic. It is denoted by **7** 24

$$[a_1, a_2, \ldots, a_n, \langle b_1, b_2, \ldots, b_m \rangle],$$

where the repeating block, $\langle b_1, b_2, \ldots, b_m \rangle$, is shown in angled brackets. The block is called the cycle of the continued fraction.

polynomial congruence A polynomial congruence is a congruence of the form $P(x) \equiv 0 \pmod{n}$, where $P(x)$ is an integral polynomial. **3** 16

prime number An integer $n \geq 2$ is said to be prime if it has no positive divisor other than itself and 1. **2** 5

prime decomposition The prime decomposition of an integer $n \geq 2$ is its unique representation as **2** 10

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r},$$

where, for $1 \leq i \leq r$, the p_i are distinct primes and k_i is a positive integer. The primes are normally listed in ascending order.

prime triplet If, of four consecutive odd integers, three are prime then they are said to form a prime triplet. **2** 24

prime quartet If, of five consecutive odd integers, four are prime then they are said to form a prime quartet. **2** 24

primitive Pythagorean triple A Pythagorean triple is a triple (x, y, z) of positive integers which give a solution of the Diophantine equation $x^2 + y^2 = z^2$. If, in addition, $\gcd(x, y) = 1$ then the triple is said to be primitive. In this case x is conventionally chosen to be the unique even member of the triple. **8** 12

primitive root The integer a is a primitive root of prime p if the successive powers of a run through all the $p - 1$ non-zero residues modulo p. **5** 29

The integer a is a primitive root of n if the successive powers of a run through a reduced set of residues for n. In this case there will be $\phi(n)$ distinct powers of a modulo n, where ϕ is Euler's ϕ-function.

pseudoprime A pseudoprime is a composite integer n with the property that n divides $2^n - 2$. **4** 8

purely periodic continued fraction A periodic continued fraction, **7** 24

$$[\langle a_1, a_2, \ldots, a_n \rangle],$$

in which the cycle begins at the first partial quotient, is said to be purely periodic.

Pythagorean equation The Pythagorean equation is the Diophantine equation $x^2 + y^2 = z^2$, requiring positive integer solutions. **8** 12

quadratic character If p is an odd prime and $\gcd(a, p) = 1$, the quadratic character of a modulo p refers to whether a is a quadratic residue or a quadratic non-residue of p. **6** 5

quadratic congruence A quadratic congruence is a polynomial congruence of degree 2; that is, it is a congruence of the form $ax^2 + bx + c \equiv 0 \pmod{n}$ where a, b and c are integers and $a \not\equiv 0 \pmod{n}$. **6** 4

quadratic residue (non-residue) If p is an odd prime and $\gcd(a, p) = 1$, then a is either a quadratic residue or a quadratic non-residue of p. If the congruence **6** 5

$$x^2 \equiv a \pmod{p}$$

has a solution, then a is a quadratic residue of p; otherwise, a is a quadratic non-residue.

rational number A rational number, expressed in its lowest terms, is a number of the form $\frac{a}{b}$ where a and b are integers, $b \geq 1$ and $\gcd(a, b) = 1$. **7** 9

reduced set of residues A reduced set of residues modulo n is a set of integers $\{a_1, a_2, \ldots, a_k\}$ each of which is relatively prime to n, no two of which are congruent modulo n, and such that every integer relatively prime to n is congruent modulo n to one of them. The number, k, of integers in a reduced set of residues is $\phi(n)$, where ϕ is Euler's ϕ-function. **5** 18

The reduced set of residues in which each integer is positive and less than or equal to n is the reduced set of least positive residues.

relatively prime Two integers a and b, not both 0, are said to be relatively prime whenever $\gcd(a, b) = 1$. **1** 25

repunit A repunit is a positive integer each of whose (decimal) digits is 1. **5** 22

residue class The residue class modulo n of an integer a consists of all integers which are congruent modulo n to a. **3** 9

simple continued fraction A continued fraction $[a_1, a_2, a_3, \ldots]$, finite or infinite, is said to be simple if each partial quotient is an integer. **7** 7

solutions of a polynomial congruence Let $S = \{b_1, b_2, \ldots, b_n\}$ be a complete set of residues modulo n. The number of solutions of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ is the number of integers $b \in S$ for which $P(b) \equiv 0 \pmod{n}$. Any solution of the congruence is congruent modulo n to one of these. **4** 19

square-free An integer $n > 1$ is said to be square-free if it is not divisible by the square of any prime. The largest exponent in the prime decomposition of a square-free integer n will be 1. **5** 33

triangular numbers The triangular number T_n, for $n \geq 1$, is the sum of the first n natural numbers: **1** 7

$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

twin primes If two consecutive odd positive integers are both prime they are said to be twin primes. **2** 22

ϕ-function For any integer $n \geq 1$, $\phi(n)$ is defined to be the number of positive integers not exceeding n which are relatively prime to n. ($\phi(1) = 1$.) **5** 18

σ function For any integer $n \geq 1$, $\sigma(n)$ is defined to be the sum of the distinct divisors of n, including 1 and n itself. ($\sigma(1) = 1$.) **5** 6

τ function For any integer ≥ 1, $\tau(n)$ is defined to be the number of distinct divisors of n, including 1 and n itself. ($\tau(1) = 1$.) **2** 13

RESULTS

Unit 1 Foundations

The Well-Ordering Principle for $\mathbb{Z}^+$

Every non-empty subset of $\mathbb{Z}^+$ has a least member. That is, if S is a non-empty subset of $\mathbb{Z}^+$ then there exists $b \in S$ such that $b \leq n$ for all $n \in S$.

Theorem 3.1 Principle of Finite Induction

If S is a set of positive integers with the following two properties:

(a) 1 is a member of S;

(b) if $k \in S$, then the next integer $k+1 \in S$;

then $S = \mathbb{Z}^+$.

Principle of Mathematical Induction

Let $P(n)$ be a proposition depending on a positive integer n. If:

(a) $P(1)$ is true;

(b) for any integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true;

then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Principle of Mathematical Induction (generalized)

Let $P(n)$ be a proposition depending on an integer n. If:

(a) $P(n_0)$ is true;

(b) for any integer $k \geq n_0$, if $P(k)$ is true then $P(k+1)$ is true;

then $P(n)$ is true for all integers $n \geq n_0$.

Second Principle of Mathematical Induction

Let $P(n)$ be a proposition depending on an integer n. If:

(a) $P(n_0)$ is true;

(b′) for any integer $k \geq n_0$, if $P(n_0)$, $P(n_0+1)$, $\ldots$, $P(k)$ are all true, then $P(k+1)$ is true;

then $P(n)$ is true for all integers $n \geq n_0$.

Theorem 4.1 The Division Algorithm

For any two integers a and b, where $b > 0$, there exist unique integers q and r such that

$$a = bq + r, \quad \text{where } 0 \leq r < b.$$

Theorem 4.2 Properties of division

Let a and b be positive integers and c and d be any integers.

(a) If $a \mid c$ then $a \mid (c + na)$ for any integer n.

(b) If $c \neq 0$ and $a \mid c$ then $a \leq |c|$.

(c) If $a \mid b$ and $b \mid a$ then $a = b$.

(d) If $a \mid b$ and $b \mid c$ then $a \mid c$.

(e) If $a \mid c$ and $a \mid d$ then $a \mid (mc + nd)$ for any integers m and n.

Theorem 4.3

Given any integers a and b, not both zero, there exist integers m and n such that

$$\gcd(a, b) = ma + nb.$$

In other words, $\gcd(a, b)$ is an integer combination of a and b.

Theorem 4.4

Integers a and b are relatively prime if, and only if, there exist integers m and n such that $1 = ma + nb$.

Theorem 4.5

For any integers a and b, not both zero, if $\gcd(a, b) = d$ then $\frac{a}{d}$ and $\frac{b}{d}$ are integers such that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. That is, the integers $\frac{a}{\gcd(a, b)}$ and $\frac{b}{\gcd(a, b)}$ are relatively prime.

Theorem 4.6

If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.

Theorem 4.7 Euclid's Lemma

If $a \mid bc$, with $\gcd(a, b) = 1$, then $a \mid c$.

Theorem 4.8

For any pair of positive integers a and b,

$$\text{lcm}(a, b) \times \gcd(a, b) = ab.$$

Result

If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Theorem 5.1 Solution of linear Diophantine equations

The linear Diophantine equation $ax + by = c$ has solutions if, and only if, $\gcd(a, b)$ divides c.

If this condition holds with $\gcd(a, b) > 1$ then division by $\gcd(a, b)$ simplifies the equation to $a'x + b'y = c'$, where $\gcd(a', b') = 1$.

If x_0, y_0 is one solution of this equation then the general solution is

$$x = x_0 + b'k, \quad y = y_0 - a'k, \quad k \in \mathbb{Z}.$$

Unit 2 Prime Numbers

Theorem 1.1

Each integer $n \geq 2$ is divisible by some prime number.

Theorem 1.2

If the integer $n \geq 2$ is composite, then it is divisible by some prime $p \leq \sqrt{n}$.

Theorem 1.3 Euclid's Lemma for prime divisors

If p is prime and p divides the product $a_1 a_2 \dots a_n$ then p divides a_i, for some integer i, where $1 \leq i \leq n$.

Corollary to Euclid's Lemma

If $p, p_1, p_2, \dots, p_n$ are primes such that

$$p \mid p_1 p_2 \dots p_n,$$

then $p = p_i$ for some i, where $1 \leq i \leq n$.

Theorem 1.4 The Fundamental Theorem of Arithmetic

Any integer $n \geq 2$ can be written uniquely in the form

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

where p_i, $i = 1, \dots, r$, are primes with $p_1 < p_2 < \dots < p_r$ and each k_i, $i = 1, \dots, r$, is a positive integer.

Theorem 2.1 Divisors of an integer

Let n be an integer greater than 1, with prime decomposition

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

Then the set of all divisors of n is the set of integers

$$\left\{ p_1^{h_1} p_2^{h_2} \dots p_r^{h_r} : 0 \leq h_i \leq k_i \text{ for } i = 1, 2, \dots, r \right\}.$$

Prime decomposition of $\gcd(m, n)$

$$\gcd(m, n) = p_1^{\min\{k_1, l_1\}} p_2^{\min\{k_2, l_2\}} \dots p_r^{\min\{k_r, l_r\}}.$$

Prime decomposition of $\operatorname{lcm}(m, n)$

$$\operatorname{lcm}(m, n) = p_1^{\max\{k_1, l_1\}} p_2^{\max\{k_2, l_2\}} \dots p_r^{\max\{k_r, l_r\}}.$$

Theorem 2.2 The formula for $\tau(n)$

For any integer $n \geq 2$, with prime decomposition

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

we have

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1).$$

Theorem 3.1 Euclid's Theorem

There are infinitely many primes.

Bertrand's Conjecture

For each integer $n \geq 2$, there exists a prime p such that $n < p < 2n$.

Theorem 3.2

Any integer of the form $4k + 3$ is divisible by a prime of this same form.

Theorem 3.3 Primes of the form $4k + 3$

There are infinitely many primes of the form $4k + 3$, where k is an integer.

Theorem 3.4 Dirichlet's Theorem

If a and b are positive integers with $\gcd(a, b) = 1$, then there are infinitely many primes of the form $ak + b$, where k is a non-negative integer.

Goldbach Conjecture

Every even integer from 6 onwards can be written as a sum of two odd primes.

The Prime Number Theorem

$$\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

Theorem 5.1 The relative primeness of consecutive Fibonacci numbers

For any positive integer n,

$$\gcd(F_{n+1}, F_n) = 1.$$

A useful relationship between Fibonacci numbers

For all integers $m \geq 2$ and $n \geq 1$,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

Theorem 5.2 Divisibility property of the Fibonacci numbers

For all integers $n > 2$, F_m is divisible by F_n if, and only if, m is divisible by n.

Unit 3 Congruence

Theorem 1.1 Properties of congruence

Let n be a fixed positive integer and let a, b, c and d be any integers. Then the following properties hold.

(a) $a \equiv a \pmod{n}$.

(b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$.

(e) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.

(f) If $a \equiv b \pmod{n}$ then $a^r \equiv b^r \pmod{n}$, for any integer $r \geq 1$.

Theorem 1.2 Congruent integers have the same remainders

$a \equiv b \pmod{n}$ if, and only if, the integers a and b have the same remainder when divided by n.

Theorem 1.3

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then

$$a \equiv b \pmod{\mathrm{lcm}(m, n)}.$$

Corollary to Theorem 1.3

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, where $\gcd(m, n) = 1$, then $a \equiv b \pmod{mn}$.

Theorem 1.4 Cancellation rule

If $ca \equiv cb \pmod{n}$ then $a \equiv b \left(\mathrm{mod}\ \frac{n}{d}\right)$, where $d = \gcd(c, n)$.

Corollary to the cancellation rule

If $ca \equiv cb \pmod{n}$, where $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Theorem 1.5 Euclid's Lemma for prime divisors

If $ab \equiv 0 \pmod{p}$ then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Theorem 2.1 Divisibility by 9 and 11

Let the integer N be written in decimal notation as $N = a_m a_{m-1} \ldots a_2 a_1 a_0$ so that the digits satisfy $0 \leq a_i \leq 9$ with $a_m \neq 0$. Then:

(a) $N \equiv a_0 + a_1 + a_2 + a_3 + \cdots + a_m \pmod{9}$;

(b) $N \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m \pmod{11}$.

Theorem 3.1

Let $P(x)$ be an integral polynomial. If $a \equiv b \pmod{n}$ then $P(a) \equiv P(b) \pmod{n}$. In particular, a is a solution of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ if, and only if, b is a solution.

Theorem 3.2 Solution of linear congruences

Consider the linear congruence $ax \equiv b \pmod{n}$.

(a) The congruence has solutions if, and only if, $\gcd(a, n)$ divides b.

(b) If $\gcd(a, n) = 1$, the congruence has a unique solution.

(c) If $\gcd(a, n) = d$ and d divides b, then the congruence has d solutions which are given by the unique solution modulo $\frac{n}{d}$ of the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right).$$

Strategy: to solve the linear congruence $ax \equiv b \pmod{n}$

1 Check that $\gcd(a, n)$ divides b. If it does not the congruence has no solutions. If it does:

2 Cancel any common divisors of all three of a, b and n. The resulting congruence has a unique solution modulo the new modulus.

The resulting coefficients (originally a and b) can then be changed by applying the remaining steps in any order, any number of times, with the goal of reaching a congruence in which the coefficient of x is 1.

3 Cancel any common divisor of the coefficients.

4 Replace either coefficient by any congruent number.

5 Multiply through the congruence by any number which is relatively prime to the modulus.

Theorem 4.1 Chinese Remainder Theorem

Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv b_1 \pmod{n_1}; \quad x \equiv b_2 \pmod{n_2}; \quad \ldots; \quad x \equiv b_r \pmod{n_r}$$

has a simultaneous solution which is unique modulo $n_1 n_2 \ldots n_r$.

Theorem 4.2

The system of linear congruences

$$x \equiv b_1 \pmod{n_1}\,;\; x \equiv b_2 \pmod{n_2}$$

has a simultaneous solution if, and only if, $\gcd(n_1, n_2)$ divides $b_2 - b_1$. If a solution exists then it is unique modulo $\text{lcm}(n_1, n_2)$.

Corollary to Theorem 4.2

The system of linear congruences

$$x \equiv b_1 \pmod{n_1}\,;\quad x \equiv b_2 \pmod{n_2}\,;\quad \ldots\;;\quad x \equiv b_r \pmod{n_r}$$

has a simultaneous solution if, and only if, $\gcd(n_i, n_j)$ divides $b_j - b_i$ for each pair i, j of suffixes. If a solution exists it is unique modulo $\text{lcm}(n_1, n_2, \ldots, n_r)$.

Unit 4 Fermat's and Wilson's Theorems

Theorem 1.1 Fermat's Little Theorem

If p is a prime and a is any integer with $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}\,.$$

Fermat's Little Theorem, an alternative formulation

If p is a prime and a is any integer,

$$a^p \equiv a \pmod{p}\,.$$

Theorem 2.1 Terminating decimals

The decimal of $\dfrac{1}{n}$ terminates if, and only if, $n = 2^r 5^s$, for some integers $r \geq 0$ and $s \geq 0$.

Theorem 2.2 The cycle length of $\dfrac{1}{p}$

The length of the cycle in the decimal of $\dfrac{1}{p}$ is equal to the order of 10 modulo p.

Theorem 2.3

If a has order c modulo p, where $p \geq 3$ is prime, and $a^k \equiv 1 \pmod{p}$ then c is a divisor of k.

In particular, c divides $p - 1$.

Theorem 3.1 Wilson's Theorem

If p is prime then $(p-1)! \equiv -1 \pmod{p}$.

Theorem 3.2 Converse of Wilson's Theorem

If $n > 1$ is an integer and $(n-1)! \equiv -1 \pmod{n}$ then n is prime.

Theorem 4.1 Lagrange's Theorem

Let p be a prime. A polynomial congruence $P(x) \equiv 0 \pmod{p}$ of degree $k \geq 1$ can have at most k solutions.

Theorem 4.2

Let b be a solution of the polynomial congruence $P(x) \equiv 0 \pmod{p}$ of degree $k \geq 1$. Then $P(x) \equiv (x-b)P_1(x) \pmod{p}$, where $P_1(x)$ is a polynomial of degree $k-1$ modulo p.

Theorem 4.3 Factorizing a polynomial modulo p

Let p be prime and let $b_1, b_2, \ldots, b_r$ be incongruent solutions of $P(x) \equiv 0 \pmod{p}$ which has degree $k \geq r$. Then

$$P(x) \equiv (x-b_1)(x-b_2)\ldots(x-b_r)P_r(x) \pmod{p},$$

where the polynomial $P_r(x)$ has degree $k-r$ modulo p.

Corollary to Theorem 4.3

For any prime p

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\ldots(x-(p-1)) \pmod{p}.$$

Theorem 4.4

If p is prime and d is a divisor of $p-1$ then the congruence

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

Unit 5 Multiplicative Functions

Divisor sum formulae for τ and σ

$$\tau(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d$$

Theorem 1.1 Equivalent definition of multiplicative functions

The function f is a multiplicative function if, and only if, for every pair, m and n, of relatively prime positive integers,

$$f(mn) = f(m)f(n).$$

Theorem 1.2 Generating new number-theoretic functions

If f is a multiplicative function, then the number-theoretic function F defined by

$$F(n) = \sum_{d|n} f(d)$$

is also multiplicative.

Corollary to Theorem 1.2

The functions τ and σ are multiplicative.

Theorem 1.3 The prime decomposition formula for σ

$$\begin{aligned}\sigma\left(p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}\right) &= \left(1+p_1+p_1^2+\cdots+p_1^{k_1}\right)\ldots\left(1+p_r+p_r^2+\cdots+p_r^{k_r}\right)\\ &= \prod_{1\leq i\leq r}\frac{p_i^{k_i+1}-1}{p_i-1}\end{aligned}$$

Theorem 2.1 Classification of even perfect numbers

If k is a positive integer such that $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ is perfect. Furthermore, every even perfect number is of this form for some positive integer k.

Theorem 2.2

If p and $2p + 1$ are primes, where $p \equiv 3 \pmod 4$, then $2p + 1$ divides M_p.

Theorem 2.3

Any prime divisor of M_p, where p is an odd prime, is of the form $2kp + 1$ for some positive integer k.

Theorem 2.4 Euler's form for an odd perfect number

If n is an odd perfect number then

$$n = p^k p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r},$$

where the p_is are distinct primes and $p \equiv k \equiv 1 \pmod 4$.

Theorem 3.1 Euler's Theorem—a generalization of FLT

If n is a positive integer and a is any integer with $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod n$.

Theorem 3.2

If the integer a has order c modulo n then $a^k \equiv 1 \pmod n$ if, and only if, k is a multiple of c. In particular the order c divides $\phi(n)$.

Repunit property 1

$$R_n = \frac{10^n - 1}{9}$$

Repunit property 2

$$R_{m+n} = R_m \times 10^n + R_n$$

Theorem 4.1 Multiplicativity of ϕ

The function ϕ is multiplicative.

Theorem 4.2 Formula for $\phi(n)$

If n has prime decomposition $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, then

$$\begin{aligned}\phi(n) &= p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

Alternative formula for $\phi(n)$

If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, then

$$\phi(n) = p_1^{k_1 - 1} p_2^{k_2 - 1} \dots p_r^{k_r - 1}(p_1 - 1)(p_2 - 1) \dots (p_r - 1).$$

If p is prime and $\gcd(a, p) = 1$ then the order of a modulo p is the least positive integer c such that $a^c \equiv 1 \pmod p$.

Theorem 4.3

$$\sum_{d|n} \phi(d) = n$$

Theorem 5.1

If a is a primitive root of n then

$$\{a, a^2, a^3, \ldots, a^{\phi(n)}\}$$

is a reduced set of residues modulo n.

Theorem 5.2

If a has order c modulo n then, for any $k \geq 1$, a^k has order

$$\frac{c}{\gcd(c,k)} \quad \text{modulo } n.$$

Corollary to Theorem 5.2

If a is a primitive root of n then a^k is also a primitive root of n if, and only if, k is relatively prime to $\phi(n)$.

Furthermore, if n has a primitive root, then it has exactly $\phi(\phi(n))$ primitive roots.

Theorem 5.3

Any integer which can be expressed as the product of two divisors which are relatively prime and each exceeding 2 does not have a primitive root.

Corollary to Theorem 5.3

If an integer n has a primitive root then it must have one of the following forms.

(a) $n = p^k$, p prime, $k \geq 1$

(b) $n = 2p^k$, p an odd prime, $k \geq 1$

Theorem 5.4

For any $k \geq 3$, 2^k does not have a primitive root.

Theorem 5.5 Integers with primitive roots

The integer n has a primitive root if, and only if, $n = 2$, 4, p^k or $2p^k$, for p an odd prime and $k \geq 1$.

Unit 6 Quadratic Reciprocity

Theorem 1.1 The quadratic residues of p

For any odd prime p there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues. The quadratic residues are congruent modulo p to the integers $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

Theorem 1.2 Euler's Criterion

Let p be an odd prime and $a \not\equiv 0 \pmod{p}$. Then a is a quadratic residue of p if, and only if, $a^{(p-1)/2} \equiv 1 \pmod{p}$ and is a quadratic non-residue of p if, and only if, $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Theorem 2.1 Properties of the Legendre symbol

Let p be an odd prime and let $a \not\equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$. Then the following properties hold.

(a) If $a \equiv b \pmod{p}$ then $(a/p) = (b/p)$.

(b) $(a^2/p) = 1$

(c) $(ab/p) = (a/p)(b/p)$

(d) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$

(e) $(-1/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$

Theorem 3.1 Gauss' Lemma

Let p be an odd prime and $a \not\equiv 0 \pmod{p}$. Let S be the set

$$S = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

consisting of the first $\dfrac{p-1}{2}$ positive multiples of a. If n denotes the number of members of S whose least positive residue modulo p exceeds $\dfrac{p}{2}$, then $(a/p) = (-1)^n$.

Theorem 3.2 The quadratic character of 2

If p is an odd prime then

$$(2/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8}, \\ -1, & \text{if } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8}. \end{cases}$$

Theorem 3.3 (Theorem 2.2 of Unit 5)

If p and $2p+1$ are both primes, where $p \equiv 3 \pmod{4}$ then $2p+1$ divides M_p.

Theorem 3.4

There are infinitely many primes of the form $4k+1$.

Theorem 3.5

There are infinitely many primes of the form $8k-1$.

Theorem 4.1 The Law of Quadratic Reciprocity

If p and q are distinct odd primes then

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

Theorem 4.2 An alternative formulation of LQR

If p and q are distinct odd primes then

$$(p/q) = \begin{cases} (q/p), & \text{if either } p \equiv 1 \pmod{4} \quad \text{or} \quad q \equiv 1 \pmod{4}, \\ -(q/p), & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Theorem 4.3

Let p be an odd prime and a an odd integer not divisible by p. Then

$$(a/p) = (-1)^{\alpha(a,p)},$$

where

$$\alpha(a,p) = \sum_{k=1}^{(p-1)/2} \text{int}\left(\frac{ka}{p}\right).$$

Theorem 4.4 The quadratic character of 3

If $p > 3$ is prime then

$$(3/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1, & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Unit 7 Continued Fractions

First continued fraction identity

$$[a_1, a_2, a_3, \ldots, a_n] = a_1 + \frac{1}{[a_2, a_3, \ldots, a_n]}$$

Theorem 1.1 Equivalence of FCFs and rational numbers

Every simple finite continued fraction has a rational value and, conversely, every rational number can be expressed as a simple finite continued fraction.

Second continued fraction identity

$$[a_1, a_2, \ldots, a_k, a_{k+1}] = [a_1, a_2, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}]$$

Theorem 1.2 The value of a finite continued fraction

Let $[a_1, a_2, \ldots, a_n]$ be any finite continued fraction. Define the *numerators* p_1, p_2, p_3, $\ldots$, p_n and the *denominators* q_1, q_2, q_3, $\ldots$, q_n of this continued fraction by:

$$\begin{array}{llll} p_1 = a_1, & p_2 = a_1 a_2 + 1; & p_k = a_k p_{k-1} + p_{k-2}, & 3 \le k \le n; \\ q_1 = 1, & q_2 = a_2; & q_k = a_k q_{k-1} + q_{k-2}, & 3 \le k \le n. \end{array}$$

Then the value of $[a_1, a_2, \ldots, a_n]$ is $\dfrac{p_n}{q_n}$.

Corollary to Theorem 1.2

Let $[a_1, a_2, \ldots, a_n]$ be any finite continued fraction and the numerators $p_1, p_2, \ldots p_n$ and denominators $q_1, q_2, \ldots, q_n$ be as defined in the theorem. Then its convergents are

$$C_k = \frac{p_k}{q_k}, \quad \text{for } k = 1, 2, \ldots, n.$$

Theorem 1.3 Properties of the convergents

Let $[a_1, a_2, \ldots, a_n]$ be any FCF, and let p_1, p_2, $\ldots$, p_n and q_1, q_2, $\ldots$, q_n be its numerators and denominators as defined in Theorem 1.2. Then we have the following properties.

(a) $p_k q_{k-1} - p_{k-1} q_k = (-1)^k$; that is,

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^k}{q_k q_{k-1}}, \quad \text{for } 2 \le k \le n.$$

(b) $p_k q_{k-2} - p_{k-2} q_k = (-1)^{k-1} a_k$; that is,

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^{k-1} a_k}{q_k q_{k-2}}, \quad \text{for } 3 \le k \le n.$$

(c) p_k and q_k are relatively prime for $k = 1, 2, \ldots, n$.

Theorem 1.4 The relative sizes of convergents

For any FCF the odd convergents form a strictly increasing sequence $C_1 < C_3 < C_5 < \cdots$, while the even convergents form a strictly decreasing sequence $C_2 > C_4 > C_6 > \cdots$. Every even convergent is greater than every odd convergent.

Theorem 2.1 Sequences of convergents converge

For any ICF $[a_1, a_2, a_3, \ldots]$ its sequence of convergents $\{C_n\}$ tends to a limit.

Corollary to Theorem 2.1

If $\{C_n\}$ is the sequence of convergents of x then, for each $n \geq 1$:

(a) x lies between C_n and C_{n+1};

(b) $\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$.

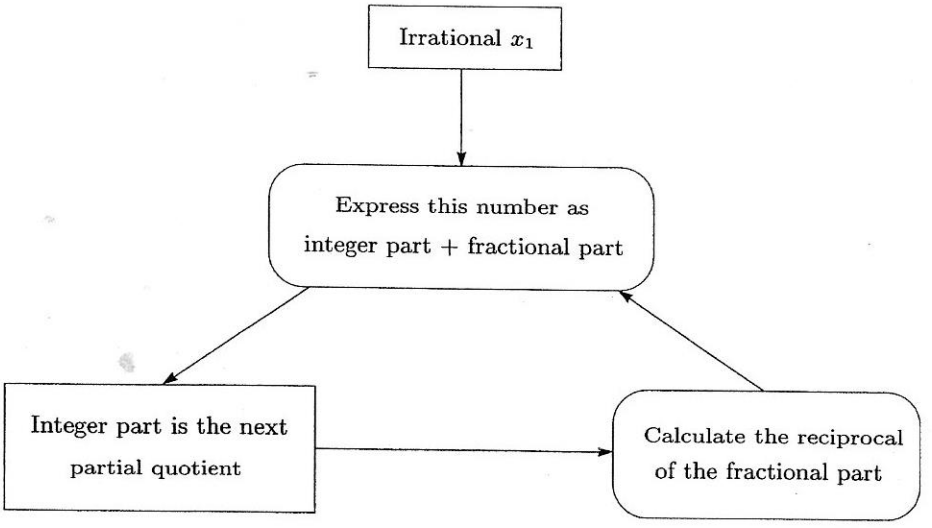
Infinite continued fraction identity

$$[a_1, a_2, a_3, \ldots] = a_1 + \frac{1}{[a_2, a_3, a_4, \ldots]}.$$

Theorem 3.1 Irrationality of ICFs

The value of any infinite simple continued fraction is an irrational number.

The Continued Fraction Algorithm



Theorem 3.2 Uniqueness of the ICF

Given any irrational number x, the ICF determined from x by the Continued Fraction Algorithm converges to x, and no other ICF converges to x.

Theorem 4.1 Accuracy of convergents

If $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \ldots$ is the sequence of convergents of x then, for all $k \geq 1$,

$$\left|x - \frac{p_{k+1}}{q_{k+1}}\right| \leq \frac{1}{q_{k+1}q_{k+2}} \leq \frac{1}{2q_k q_{k+1}} < \left|x - \frac{p_k}{q_k}\right|.$$

Corollary to Theorem 4.1

For all $k \geq 1$ the convergent $\frac{p_k}{q_k}$ of x satisfies

$$\frac{1}{2q_kq_{k+1}} < \left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_kq_{k+1}}.$$

Theorem 4.2

Let $\frac{p_n}{q_n}$ be the nth convergent of the irrational number x, and let $\frac{a}{b}$ be any rational number with $0 < b < q_{n+1}$. Then, for $n > 1$,

$$|q_nx - p_n| \leq |bx - a|,$$

the equality holding only if $a = p_n$ and $b = q_n$.

Corollary to Theorem 4.2 Convergents are best approximations

Let $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ be the convergents of the irrational number x. Then, for any rational number $\frac{a}{b}$ with $1 \leq b \leq q_n$

$$\left|x - \frac{p_n}{q_n}\right| \leq \left|x - \frac{a}{b}\right|,$$

the equality holding only if $a = p_n$ and $b = q_n$.

Theorem 4.3 Which rationals are convergents?

If the rational number $\frac{a}{b}$ satisfies

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$$

then $\frac{a}{b}$ is a convergent of x.

Unit 8 Diophantine Equations

Theorem 1.1 Solutions of Pell's equation are convergents

If $x = a$, $y = b$ is a positive solution of $x^2 - ny^2 = 1$ then $\frac{a}{b}$ is a convergent of $\sqrt{n}$.

Theorem 1.2 Solution of Pell's equation

If the continued fraction of $\sqrt{n}$ has cycle length s then

$$p_{rs}^2 - nq_{rs}^2 = (-1)^{rs}; \quad r = 1, 2, 3, \ldots,$$

and all solutions of

$$x^2 - ny^2 = \pm 1$$

are given in this way.

Theorem 1.3 All solutions from a fundamental solution

Let $x = x_1$, $y = y_1$ be the fundamental solution of $x^2 - ny^2 = 1$. Then, for each integer $k \geq 1$, $x = x_k$, $y = y_k$ is also a solution, where the positive integers x_k and y_k are given by

$$x_k + y_k\sqrt{n} = \left(x_1 + y_1\sqrt{n}\right)^k.$$

Conversely, the solutions given in this way are the only positive solutions.

Theorem 1.4

Suppose that the ICF of $\sqrt{n}$ has a cycle of odd length s. Let $x_1 = p_s$, $y_1 = q_s$, where the convergent $C_s = \dfrac{p_s}{q_s}$, and let x_k and y_k be given by

$$x_k + y_k\sqrt{n} = \left(x_1 + y_1\sqrt{n}\right)^k.$$

Then, for all integers $k \geq 1$, $x = x_{(2k-1)s}$, $y = y_{(2k-1)s}$ is a solution of $x^2 - ny^2 = -1$ and $x = x_{2ks}$, $y = y_{2ks}$ is a solution of $x^2 - ny^2 = 1$. Moreover, all solutions of $x^2 - ny^2 = \pm 1$ are given in this way.

Theorem 2.1 Primitive solutions of the Pythagorean equation

The primitive Pythagorean triples are the triples

$$(2mn,\ m^2 - n^2,\ m^2 + n^2),$$

where m and n are relatively prime positive integers of opposite parity and with $m > n$.

Corollary to Theorem 2.1 All solutions of the Pythagorean equation

The Pythagorean triples (x, y, z) are given by

$$x = 2kmn, \quad y = k(m^2 - n^2), \quad z = k(m^2 + n^2),$$

where $k \geq 1$ is any integer and m and n are relatively prime positive integers with opposite parity and $m > n$.

Theorem 3.1

The Diophantine equation $x^4 + y^4 = z^2$ has no positive solutions.

Corollary to Theorem 3.1

The Diophantine equation $x^4 + y^4 = z^4$ has no positive solutions.

Theorem 3.2

The Diophantine equation $x^4 + 4y^4 = z^2$ has no positive solution.

Corollary to Theorem 3.2

The Diophantine equation $x^4 - y^4 = z^2$ has no positive solution.

Important identity for two squares

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

Theorem 4.1 Primes expressed as a sum of two squares

A prime p can be expressed as a sum of two squares if, and only if, $p = 2$ or $p \equiv 1 \pmod 4$.

Theorem 4.2 Uniqueness of representation

The expression of a prime of form $4k + 1$ as a sum of two squares is unique except for the order of the two summands.

Theorem 4.3 Sums of two squares

A positive integer n can be expressed as a sum of two squares if, and only if, each of its prime divisors of the form $4k + 3$, if any, occurs to an even power.

Theorem 4.4 Sums of three squares

A positive integer can be expressed as a sum of three squares if, and only if, it is not of the form $4^n(8m+7)$ for some $n \geq 0$, $m \geq 0$.

Theorem 4.5 Lagrange's Four Square Theorem

Every positive integer can be expressed as a sum of four squares.

Theorem 4.6 Waring's Problem

For each integer $k \geq 2$ there exists a positive integer $g(k)$ such that every positive integer can be expressed as a sum of at most $g(k)$ kth powers.

APPENDIX: TABLE OF PRIMES

The following table lists all the odd integers up to 3999, excluding the multiples of 5. The entry 'P' in the table indicates that the number is prime. Otherwise the smallest prime divisor of the number is given. The numbers are arranged in blocks of 100, with the units digit at the head of the column and the numbers of 10's in the left-hand column.

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
0		P	P	3	50	3	P	3	P	100	7	17	19	P	150	19	3	11	3
1	P	P	P	P	51	7	3	11	3	101	3	P	3	P	151	P	17	37	7
2	3	P	3	P	52	P	P	17	23	102	P	3	13	3	152	3	P	3	11
3	P	3	P	3	53	3	13	3	7	103	P	P	17	P	153	P	3	29	3
4	P	P	P	7	54	P	3	P	3	104	3	7	3	P	154	23	P	7	P
5	3	P	3	P	55	19	7	P	13	105	P	3	7	3	155	3	P	3	P
6	P	3	P	3	56	3	P	3	P	106	P	P	11	P	156	7	3	P	3
7	P	P	7	P	57	P	3	P	3	107	3	29	3	13	157	P	11	19	P
8	3	P	3	P	58	7	11	P	19	108	23	3	P	3	158	3	P	3	7
9	7	3	P	3	59	3	P	3	P	109	P	P	P	7	159	37	3	P	3
10	P	P	P	P	60	P	3	P	3	110	3	P	3	P	160	P	7	P	P
11	3	P	3	7	61	13	P	P	P	111	11	3	P	3	161	3	P	3	P
12	11	3	P	3	62	3	7	3	17	112	19	P	7	P	162	P	3	P	3
13	P	7	P	P	63	P	3	7	3	113	3	11	3	17	163	7	23	P	11
14	3	11	3	P	64	P	P	P	11	114	7	3	31	3	164	3	31	3	17
15	P	3	P	3	65	3	P	3	P	115	P	P	13	19	165	13	3	P	3
16	7	P	P	13	66	P	3	23	3	116	3	P	3	7	166	11	P	P	P
17	3	P	3	P	67	11	P	P	7	117	P	3	11	3	167	3	7	3	23
18	P	3	11	3	68	3	P	3	13	118	P	7	P	29	168	41	3	7	3
19	P	P	P	P	69	P	3	17	3	119	3	P	3	11	169	19	P	P	P
20	3	7	3	11	70	P	19	7	P	120	P	3	17	3	170	3	13	3	P
21	P	3	7	3	71	3	23	3	P	121	7	P	P	23	171	29	3	17	3
22	13	P	P	P	72	7	3	P	3	122	3	P	3	P	172	P	P	11	7
23	3	P	3	P	73	17	P	11	P	123	P	3	P	3	173	3	P	3	37
24	P	3	13	3	74	3	P	3	7	124	17	11	29	P	174	P	3	P	3
25	P	11	P	7	75	P	3	P	3	125	3	7	3	P	175	17	P	7	P
26	3	P	3	P	76	P	7	13	P	126	13	3	7	3	176	3	41	3	29
27	P	3	P	3	77	3	P	3	19	127	31	19	P	P	177	7	3	P	3
28	P	P	7	17	78	11	3	P	3	128	3	P	3	P	178	13	P	P	P
29	3	P	3	13	79	7	13	P	17	129	P	3	P	3	179	3	11	3	7
30	7	3	P	3	80	3	11	3	P	130	P	P	P	7	180	P	3	13	3
31	P	P	P	11	81	P	3	19	3	131	3	13	3	P	181	P	7	23	17
32	3	17	3	7	82	P	P	P	P	132	P	3	P	3	182	3	P	3	31
33	P	3	P	3	83	3	7	3	P	133	11	31	7	13	183	P	3	11	3
34	11	7	P	P	84	29	3	7	3	134	3	17	3	19	184	7	19	P	43
35	3	P	3	P	85	23	P	P	P	135	7	3	23	3	185	3	17	3	11
36	19	3	P	3	86	3	P	3	11	136	P	29	P	37	186	P	3	P	3
37	7	P	13	P	87	13	3	P	3	137	3	P	3	7	187	P	P	P	P
38	3	P	3	P	88	P	P	P	7	138	P	3	19	3	188	3	7	3	P
39	17	3	P	3	89	3	19	3	29	139	13	7	11	P	189	31	3	7	3
40	P	13	11	P	90	17	3	P	3	140	3	23	3	P	190	P	11	P	23
41	3	7	3	P	91	P	11	7	P	141	17	3	13	3	191	3	P	3	19
42	P	3	7	3	92	3	13	3	P	142	7	P	P	P	192	17	3	41	3
43	P	P	19	P	93	7	3	P	3	143	3	P	3	P	193	P	P	13	7
44	3	P	3	P	94	P	23	P	13	144	11	3	P	3	194	3	29	3	P
45	11	3	P	3	95	3	P	3	7	145	P	P	31	P	195	P	3	19	3
46	P	P	P	7	96	31	3	P	3	146	3	7	3	13	196	37	13	7	11
47	3	11	3	P	97	P	7	P	11	147	P	3	7	3	197	3	P	3	P
48	13	3	P	3	98	3	P	3	23	148	P	P	P	P	198	7	3	P	3
49	P	17	7	P	99	P	3	P	3	149	3	P	3	P	199	11	P	P	P

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
200	3	P	3	7	250	41	P	23	13	300	P	3	31	3	350	3	31	3	11
201	P	3	P	3	251	3	7	3	11	301	P	23	7	P	351	P	3	P	3
202	43	7	P	P	252	P	3	7	3	302	3	P	3	13	352	7	13	P	P
203	3	19	3	P	253	P	17	43	P	303	7	3	P	3	353	3	P	3	P
204	13	3	23	3	254	3	P	3	P	304	P	17	11	P	354	P	3	P	3
205	7	P	11	29	255	P	3	P	3	305	3	43	3	7	355	53	11	P	P
206	3	P	3	P	256	13	11	17	7	306	P	3	P	3	356	3	7	3	43
207	19	3	31	3	257	3	31	3	P	307	37	7	17	P	357	P	3	7	3
208	P	P	P	P	258	29	3	13	3	308	3	P	3	P	358	P	P	17	37
209	3	7	3	P	259	P	P	7	23	309	11	3	19	3	359	3	P	3	59
210	11	3	7	3	260	3	19	3	P	310	7	29	13	P	360	13	3	P	3
211	P	P	29	13	261	7	3	P	3	311	3	11	3	P	361	23	P	P	7
212	3	11	3	P	262	P	43	37	11	312	P	3	53	3	362	3	P	3	19
213	P	3	P	3	263	3	P	3	7	313	31	13	P	43	363	P	3	P	3
214	P	P	19	7	264	19	3	P	3	314	3	7	3	47	364	11	P	7	41
215	3	P	3	17	265	11	7	P	P	315	23	3	7	3	365	3	13	3	P
216	P	3	11	3	266	3	P	3	17	316	29	P	P	P	366	7	3	19	3
217	13	41	7	P	267	P	3	P	3	317	3	19	3	11	367	P	P	P	13
218	3	37	3	11	268	7	P	P	P	318	P	3	P	3	368	3	29	3	7
219	7	3	13	3	269	3	P	3	P	319	P	31	23	7	369	P	3	P	3
220	31	P	P	47	270	37	3	P	3	320	3	P	3	P	370	P	7	11	P
221	3	P	3	7	271	P	P	11	P	321	13	3	P	3	371	3	47	3	P
222	P	3	17	3	272	3	7	3	P	322	P	11	7	P	372	61	3	P	3
223	23	7	P	P	273	P	3	7	3	323	3	53	3	41	373	7	P	37	P
224	3	P	3	13	274	P	13	41	P	324	7	3	17	3	374	3	19	3	23
225	P	3	37	3	275	3	P	3	31	325	P	P	P	P	375	11	3	13	3
226	7	31	P	P	276	11	3	P	3	326	3	13	3	7	376	P	53	P	P
227	3	P	3	43	277	17	47	P	7	327	P	3	29	3	377	3	7	3	P
228	P	3	P	3	278	3	11	3	P	328	17	7	19	11	378	19	3	7	3
229	29	P	P	11	279	P	3	P	3	329	3	37	3	P	379	17	P	P	29
230	3	7	3	P	280	P	P	7	53	330	P	3	P	3	380	3	P	3	13
231	P	3	7	3	281	3	29	3	P	331	7	P	31	P	381	37	3	11	3
232	11	23	13	17	282	7	3	11	3	332	3	P	3	P	382	P	P	43	7
233	3	P	3	P	283	19	P	P	17	333	P	3	47	3	383	3	P	3	11
234	P	3	P	3	284	3	P	3	7	334	13	P	P	17	384	23	3	P	3
235	P	13	P	7	285	P	3	P	3	335	3	7	3	P	385	P	P	7	17
236	3	17	3	23	286	P	7	47	19	336	P	3	7	3	386	3	P	3	53
237	P	3	P	3	287	3	13	3	P	337	P	P	11	31	387	7	3	P	3
238	P	P	7	P	288	43	3	P	3	338	3	17	3	P	388	P	11	13	P
239	3	P	3	P	289	7	11	P	13	339	P	3	43	3	389	3	17	3	7
240	7	3	29	3	290	3	P	3	P	340	19	41	P	7	390	47	3	P	3
241	P	19	P	41	291	41	3	P	3	341	3	P	3	13	391	P	7	P	P
242	3	P	3	7	292	23	37	P	29	342	11	3	23	3	392	3	P	3	P
243	11	3	P	3	293	3	7	3	P	343	47	P	7	19	393	P	3	31	3
244	P	7	P	31	294	17	3	7	3	344	3	11	3	P	394	7	P	P	11
245	3	11	3	P	295	13	P	P	11	345	7	3	P	3	395	3	59	3	37
246	23	3	P	3	296	3	P	3	P	346	P	P	P	P	396	17	3	P	3
247	7	P	P	37	297	P	3	13	3	347	3	23	3	7	397	11	29	41	23
248	3	13	3	19	298	11	19	29	7	348	59	3	11	3	398	3	7	3	P
249	47	3	11	3	299	3	41	3	P	349	P	7	13	P	399	13	3	7	3

CUMULATIVE INDEX OF UNITS

abundant **5** 34
accuracy of convergents **7** 33
algebraic numbers **8** 19
amicable pair **5** 34
arithmetic functions **5** 5
arithmetic progression **1** 7
arithmetic series **1** 7

basis for the induction **1** 15
Bertrand's Conjecture **2** 16
best approximations **7** 36

cancellation rule **3** 13
casting out nines **3** 14
Chinese Remainder Theorem **3** 23
classification of even perfect numbers **5** 11
complete set of residues **3** 9
composite **2** 5
congruence class **3** 9
congruent modulo n **3** 6
consecutive composite integers **2** 23
Continued Fraction Algorithm **7** 26
convergent **7** 11
converse of Wilson's Theorem **4** 18
coprime **1** 25
Corollary to Euclid's Lemma **2** 9
cycle **4** 10
cycle length **4** 10
cycle of a periodic ICF **7** 24

deficient **5** 34
degree of a polynomial congruence **4** 22
degree of a polynomial modulo n **4** 22
denominators **7** 12
density of primes **2** 25
descent step **8** 20
Diophantine equation **1** 34
Dirichlet's Theorem **2** 19
discriminant **6** 5
divides **1** 22
divisibility by 11 **3** 15
divisibility by 9 **3** 15
Division Algorithm **1** 20
divisor **1** 22
divisor sum formulas for τ and σ **5** 6
divisors of an integer **2** 11

equivalence of FCFs and rational numbers **7** 9
equivalent congruence **3** 20
Euclid's Elements **8** 13
Euclid's Lemma **1** 26
Euclid's Lemma for prime divisors **2** 8, **3** 14
Euclid's Theorem **2** 15
Euclidean Algorithm **1** 32
Euler's ϕ-function **5** 18
Euler's Criterion **6** 7
Euler's Theorem **5** 19
even convergents **7** 17

factor **1** 22
factorizing a polynomial congruence **4** 23
FCF **7** 8
Fermat numbers **5** 16
Fermat's Last Theorem **8** 18
Fermat's Little Theorem **4** 6
Fermat's Little Theorem, an alternative formulation **4** 7
Fibonacci numbers **2** 28
Fibonacci numbers, divisibility property **2** 31
Fibonacci numbers, relative primeness of consecutive numbers **2** 29
Fibonacci primes **2** 28
Fibonacci sequence **2** 27
finite continued fraction **7** 7
formula for $\phi(n)$ **5** 26
formula for σ **5** 10
formula for $\tau(n)$ **2** 13
fractional part **7** 27
function τ **2** 13
fundamental solution **8** 9
Fundamental Theorem of Arithmetic **2** 10

Gauss' Lemma **6** 15
geometric series **1** 16
Goldbach's Conjecture **2** 24
golden ratio **7** 5
greatest common divisor **1** 23

heptagonal numbers **1** 10
heptagonal-based pyramidal numbers **1** 12
hexagonal numbers **1** 9
highest common factor **1** 23
hypoteneuse **8** 12

ICF **7** 20
ideal prime divisors **8** 19
important identity for four squares **8** 33
important identity for two squares **8** 25
incongruent modulo n **3** 6
induction hypothesis **1** 15
induction step **1** 15
infinite continued fraction **7** 20
integer combination **1** 24
integral polynomial **3** 16
irrationality of ICFs **7** 26

Jacobi symbol **6** 28

Lagrange's Four Square Theorem **8** 33
Lagrange's Theorem **4** 22
Law of Quadratic Reciprocity **6** 21
leading term of a polynomial **4** 22
least absolute residues **3** 9
least common multiple **1** 28
least positive residues **3** 9
Legendre symbol, (a/p) **6** 12
length of a cycle **4** 10
linear congruence **3** 18
linear Diophantine equation **1** 34
LQR **6** 21

LQR an alternative formulation **6** 21

Mathematical Induction **1** 15
Mersenne number **5** 12
Mersenne prime **5** 12
method of infinite descent **8** 20
multiple **1** 22
multiplicative functions **5** 7

non-negative integers **1** 33
non-terminating decimals **4** 10
number of solutions of a polynomial congruence **3** 17
number-theoretic functions **5** 5
numerators **7** 12

octagonal numbers **1** 10
odd convergents **7** 17
order of an integer modulo a prime **4** 13
order of an integer to a composite modulus **5** 20

parity **8** 13
partial quotients **7** 7
parts of a positive integer **5** 11
Pell's equation **8** 5
pentagonal numbers **1** 9
perfect number **5** 11
perfect squares **1** 8
periodic **7** 24
polygonal numbers **1** 10
polynomial congruence **3** 16, **4** 19
prime **2** 5
prime decomposition **2** 10
prime decomposition of $\gcd(m,n)$ **2** 12
prime decomposition of $\mathrm{lcm}(m,n)$ **2** 13
prime number theorem **2** 26
prime quartets **2** 24
prime triplets **2** 24
primes generated by polynomials **2** 20
primes in arithmetic progression **2** 16
primes of the form $4k+3$ **2** 18
primitive Pythagorean triple **8** 12
primitive root **4** 13, **5** 29
Principle of Finite Induction **1** 14
Principle of Mathematical Induction **1** 15
Principle of Mathematical Induction (generalized) **1** 16
proper fraction **4** 16
properties of congruence **3** 7
properties of the convergents **7** 16
pseudoprimes **4** 8

purely periodic **7** 24
pyramidal numbers **1** 11
Pythagorean equation **8** 12
Pythagorean triple **8** 12

quadratic character **6** 5
quadratic character of 2, $(2/p)$ **6** 18
quadratic character of 3, $(3/p)$ **6** 27
quadratic congruence **4** 18, **6** 4
quadratic irrationals **7** 30
quadratic non-residue **6** 5
quadratic residue **6** 5

rational approximations **7** 32
rational number **7** 9
reduced set of least positive residues modulo n **5** 18
reduced set of residues modulo n **5** 18
regular primes **8** 19
relatively prime **1** 25
repunit **5** 22
residue class **3** 9
ring **8** 19

Second Principle of Mathematical Induction **1** 18
sieve of Eratosthenes **2** 7
simple continued fraction **7** 7
simple infinite continued fraction **7** 20
simultaneous linear congruences **3** 22
simultaneous solution **3** 23
size of the nth prime **2** 15
solution by exhaustion **3** 18
solutions of a polynomial congruence **4** 19
square number **1** 8
square-based pyramidal numbers **1** 11
square-free **5** 33
squares **1** 8
sums of squares **8** 24
sums of three squares **8** 32

terminating decimals **4** 10
triangle-based pyramidal numbers **1** 11
triangular numbers **1** 7
twin primes **2** 22

value of $\gcd(n,p)$ **2** 8
value of a continued fraction **7** 7
value of an infinite continued fraction **7** 21

Well-Ordering Principle **1** 13
Wilson's Theorem **4** 17

Printed in the United Kingdom by
The Open University